



Pakistan Telecom Authority HQs., F-5/1, Islamabad

PTA Cyber Security Advisory No: 078

28-April-2020

Name: Palo Alto Networks Insecure temporary file Vulnerability (CVE-2020-1991)

Threat Classification: Privilege Escalation

Affected Systems: Affects the following Palo Alto Networks Traps product:

- Traps 5.0 versions earlier than 5.0.8 on Windows
- Traps 6.1 versions earlier than 6.1.4 on Windows

Summary:

An insecure temporary file vulnerability exists in Palo Alto Networks Traps that allows a local authenticated Windows user to escalate privileges or overwrite system files. This issue does not affect Cortex XDR 7.0 and also does not affect Traps for Linux or MacOS.

| | |
|----------------------------|----------------------|
| Attack Severity | HIGH |
| Attack Type | Privilege Escalation |
| Privileges required | None |

For further details, please visit following vendor official link:

<https://security.paloaltonetworks.com/CVE-2020-1991>

Recommendations:

- This vulnerability is fixed in Traps 5.0.8, 6.1.4 and later versions. Please visit following official website link for the detailed release notes and remediation of the aforementioned vulnerability:

<https://docs.paloaltonetworks.com/traps.html>

- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.
- In all cases, also ensure that devices to be upgraded to new release meet the requirements set by the vendor.
- Whenever required, access the system with minimal access rights and privileges.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.

